240-WP-005-001

Security Access Control Management (SACM) Product Trade Study and Technical Evaluation

White Paper

February 2004

Prepared Under Contract NAS5-60000

RESPONSIBLE AUTHOR

Kenneth Simmons /s/ 2/11/04

Kenneth Simmons, Systems Engineer Date
EOSDIS Core System Project

RESPONSIBLE OFFICE

Mary Armstrong /s/ 2/16/04

Mary Armstrong, Systems Engineering Date
EOSDIS Core System Project

Raytheon Company
Upper Marlboro, Maryland

This page intentionally left blank.

Abstract

This white paper presents the trade study and evaluation results of alternatives for a Security Access Control Management (SACM) Commercial-off the-Shelf (COTS) product. The COTS product recommended in this paper will continue to ensure that ECS meets the requirements set-forth in the NASA Security Policy Guideline (NPG 2810.1), while improving the current ECS security access control management process.

Keywords: security access control management, trade study, NPG 2810.1.

This page intentionally left blank.

Contents

6. SACM Operational Impact Objectives

7. Security Access Control Management Product Trade Study

8. Security Access Control Management Product Cost Comparison

9. Security Access Control Management Product Technical Evaluation

10. Recommendation

11. Future Trade Study and Evaluation

List of Tables

List of Figures

This page intentionally left blank.

1. Introduction

1.1 Identification

This white paper identifies and describes the trade study and technical evaluation, for the selection of a Security Access Control Management (SACM) COTS product. It also provides a recommendation to NASA for the COTS product.

1.2 Scope

The scope is restricted to UNIX administrative privilege management, system monitoring, login and password management within the ECS Core System environment.

1.3 Purpose and Objectives

This white paper presents the trade study and evaluation results of alternatives for a Security Access Control Management (SACM) Commercial-off the-Shelf (COTS) product. The COTS product recommended in this white paper will continue to ensure that ECS meets the requirements set-forth in the NASA Security Policy Guideline (NPG 2810.1), while improving the current ECS security access control management process.

1.4 Document Organization

This paper is organized as follows:

Section 1 States the purpose, organization, point of contacts.

Section 2 Describes the background and the technical approach used in the evaluation of Security Access Control Management product.

Section 3 Contains the ECS security requirements in the F&PRS and the derived requirements recently developed during this study for the SACM.

Section 4 provides an overview of the current ECS security architecture.

Section 5 provides the operational scenarios used to derive the SACM requirements.

Section 6 provides the operational impact of the COTS product on the ECS environment.

Section 7 provides the COTS product trade study analysis

Section 8 provides the COTS product cost comparison.

Section 9 provides the COTS product technical evaluation test scenarios and results.

Section 10 provides the SACM COTS product recommendation.

1.5 Review and Approval

This Technical Paper is an informal document approved at the Office Manager level. It does not require formal Government review or approval; however, it is submitted with the intent that review and comments will be forthcoming.

Questions regarding technical information contained within this Paper should be addressed to the following ECS contacts:

•ECS Contacts

Kenneth Simmons; Systems Engineering Department; (301) 925-0896; ksimmons@eos.east.hitc.com

Byron Peters; System Engineering Department; (301) 925-0350; Bpeters@eos.east.hitc.com

2. Background and Need for SACM Product

The ECS program is currently performing at an adequate level of security administration as stated in the ECS F&PRS, Level 3 Requirements, ECS Security Plan, Proposal for Security Requirement Technical Volume, 803-RD-031-001, dated December 2000,and NASA Policy Security Guideline NPG 2810.1. We are still largely dependent on freeware products for host-level security applications. ANL-password, Tripwire and the UNIX operating system itself are still the foundation of the host-level defense.

The ECS program has a first class firewall system that provides an unsurpassed level of protection from external threats. The security administrators at each DAAC, the SMC, the PVC and the VATC have been extremely diligent in managing their systems, as exemplified by very low vulnerability scores subsequent to site security scans. As a result of the diligent effort by the security administrator, all of the ECS facilities are operating in the "green".

Interactive access to DAAC systems, especially from the Internet, is strictly limited to Secure Shell (ssh). The user access to "r" commands has been eliminated at the DAACs/SMC and the use of telnet has either been eliminated or is only useable from within a DAAC. The supported commercial version of F-Secure SSH is used in ECS.

From an internal threat perspective, ECS is using operating system level functionality combined with the host-based intrusion detection capability of Tripwire 1.3. This has been sufficient historically. However, with an ever-increasing need of government systems to improve defensive capabilities, constant improvements must be made. These days of constant levels of threats against U.S Government systems, Raytheon is continuing to be proactive in combating such threats. We are continuing to implement and improve procedures and practices to ensure the security, integrity, and continued operation of the ECS and the information it stores and processes.

2.1 Technical Approach

ECS systems engineering has undertaken this effort to reduce risk associated with the increasing need for more robust security access control management. In the first step of this effort, ECS engineers identified all of the requirements that pertain to security access control management. The requirements identified were gathered from a variety of different sources such as NASA's ECS Functional and Performance Requirements Specification (F&PRS), ECS Level 3 Requirements, NASA' Policy Guideline 2810.1, and the Proposal for Security Requirement Technical Volume, 803-RD-031-001, dated December 2000. Other documents used in the development of the technical approach include Tivoli white paper dated February 25, 2003, and derived access control management requirements. Both the Tivoli white paper and the derived requirements provided the basis of the recommendation to the government.

Next, ECS engineers performed an analysis of the requirements identified in the above-mentioned sources. Each requirement was decomposed and allocated to a functional or performance category.

Several security access control management COTS products were identified as possible solutions. ECS engineers performed an evaluation to identify a solution that meets the requirements.

The evaluation team obtained an evaluation copy of the candidates COTS products and configured them into the ECS COTS product evaluation environment. In this environment, the engineers performed a variety of tests were performed to determine the compatibility, suitability, and adaptability of the product into the ECS environment.

3. Security Management Access Control Management (SACM) Requirements

Figure 3-1 depicts the flow diagram for the development of the security access control management white paper.

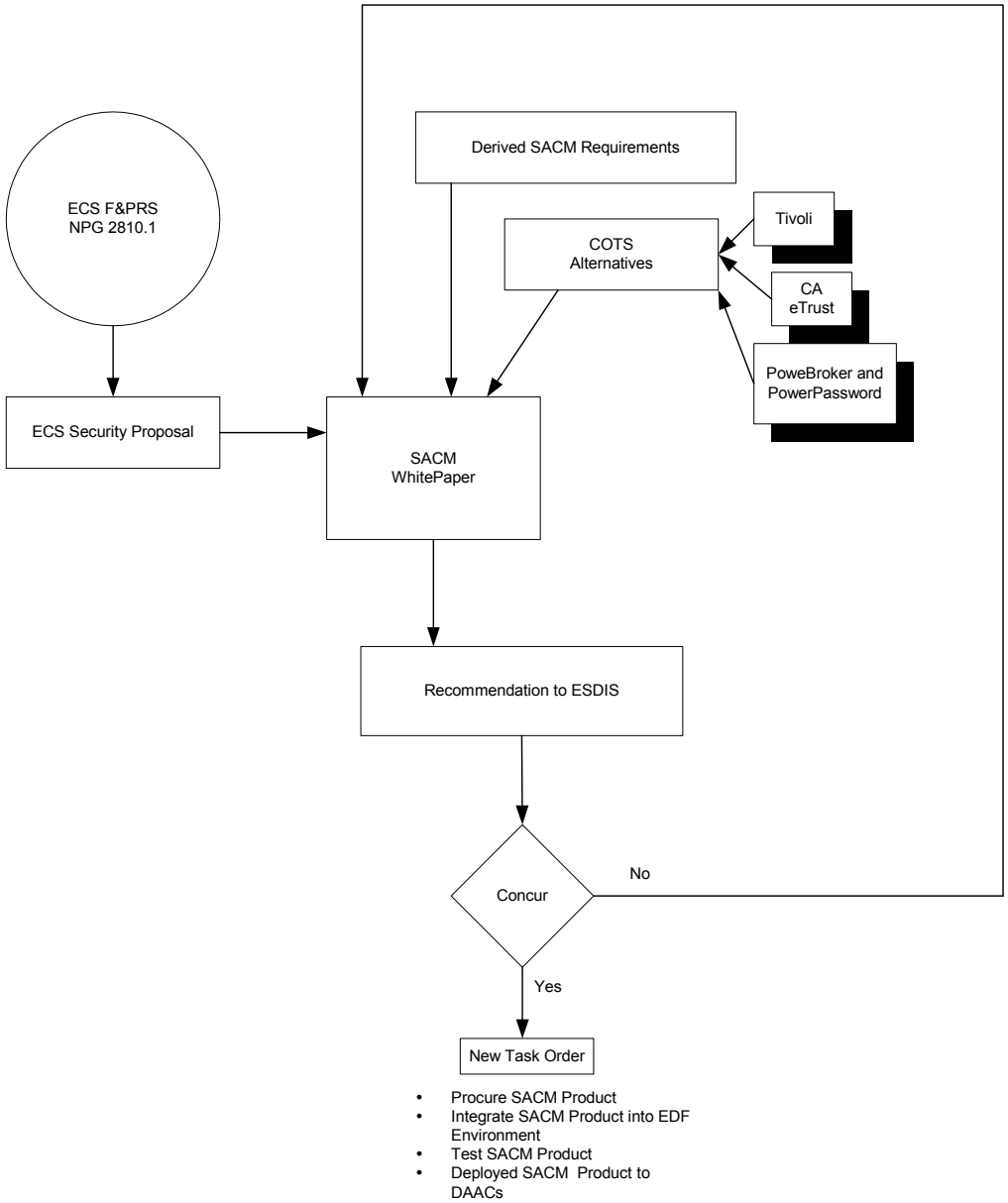

Figure 3-1. SACM White paper Flow Diagram

3.1 F&PRS Security Requirements

Table 3.1-1 provides a list of F&PRS requirements relevant to security access control management (SACM).

Table 3.1-1. F&PRS Requirements (1 of 2)

F&PRS Requirement ID	F&PRS Requirement Text
EOSD1990	The ECS system shall employ security measures and techniques for all applicable security disciplines which are identified in the following documents • OMB Circular #A-130 • NPD 1600.2A • NPG 2810.1
EOSD2100	The ECS technical security policy planning shall be comprehensive and shall cover the following areas: • ECS communications, network access, control, and monitoring • Data protection controls • Account/privilege management and user session tailoring • Restart/recovery • Security audit trail generation • Security analysis and reporting • Risk analysis
EOSD2400	The ECS shall provide data protection based on 'Information
EOSD2430	ECS database access and manipulation shall accommodate control of user access and update of security controlled data.
EOSD2440	ECS data base integrity including prevention of data loss and corruption shall be maintained. EOSD2480
EOSD2480	ECS elements shall require unique sessions when security controlled data are being manipulated
EOSD2510	Unsuccessful access attempt to security controlled data by unauthorized users/processes

Table 3.1-1. F&PRS Requirements (2 of 2)

F&PRS Requirement ID	F&PRS Requirement Text
EOSD2550	The ECS shall limit use of master passwords or use of a single password for large organizations requiring access to a mix of security controlled and non-sensitive data.
EOSD2555	The ECS shall maintain confidentiality of user product request and accounts.
EOSD2620	ECS shall disconnect an operator after a predetermined number of unsuccessful attempts to access data.
EOSD2650	The ECS shall report detected security violations to the SMC.
EOSD2990	The ECS shall support the recovery from a system failure due to a loss in the integrity of the ECS data or a catastrophic violation of the security system.
EOSD3000	The ECS shall provide for security safeguards to cover unscheduled system shutdown (aborts) and subsequent restarts, as well as for scheduled system shutdown and operational startup.
EOSD3200	A minimum of one backup which is maintained in a separate physical location (i.e., different building) shall be maintained for ECS software and key data items (including security audit trails and logs).
EOSD3220	All media shall be handled and stored in protected areas with environmental and accounting procedures applied.

3.2 NASA Policy Guideline 2810.1 (SACM) Requirements

Table 3.2-1 provides a list of NASA Policy Guideline 2810.1 requirements that pertain to security access control management (SACM).

Table 3.2-1. NASA NPG 2810.1 Requirements (1 of 4)

NPG 2810.1 Requirement ID	High Level Requirement Text	Detailed Requirement Text
A.6.1.1.	Critical System Files Protection Critical system files are those that are integral to the operating system, system security mechanisms, or key system services. Corrupting these files would damage the integrity of the system. Management will implement a process that accomplishes the following:	Controls file access Identifies and protects critical system files Restricts access to critical system files to authorized users Restricts access to password files Reviews critical system file protection at least annually

Table 3.2-1. NASA NPG 2810.1 Requirements (2 of 4)

NPG 2810.1 Requirement ID	High Level Requirement Text	Detailed Requirement Text
A.6.2.1.	User ID Approval Process/Privileges A management control process will be implemented to ensure that all requests for user ID's are reviewed and approved by NASA line management. A list of personnel who are authorized to approve the user ID's will be furnished to the appropriate user-ID administrator. Management will implement a process that accomplishes the following:	Requires all individuals requesting a user ID to complete the appropriate request form and sign a statement of responsibility indicating their understanding of the requirements for using and safeguarding the information to which the assigned user ID is granted access Retains the statement of responsibility by user ID management for a minimum of 1 year
A.6.2.2.	Group User ID's Group user ID's are discouraged because individual accountability is lost. However, if the system is configured such that group user ID's must be used, then management will implement a process that accomplishes the following:	Restricts group user ID's to the minimum number necessary to conduct system operations
A.6.2.4.	Disposition of Unused User ID's Management will ensure that proper disposition is made of all unused user ID's. User ID disposition uses password lifetime (i.e., the number of days before users receive reminders to change their passwords) as the metric for user-ID-deletion decisions. The table below identifies the maximum lifetimes (in calendar days) before a user ID is removed from the system.	Number of days before user receives reminders to change password (90 day) Number of days that user will be reminded to change password (+30 days) Number of days until user ID is suspended if user does not change password (120 total days) Number of days until user ID is removed from the system (240 total days)
A.6.2.6	Notification Upon Termination In accordance with the following time limits, a user's supervisor will notify the manager of all systems on which the user holds a user ID when that individual is terminated, retires, or is transferred	Within 2 working days of the termination
A.6.3.	Passwords Users are responsible for any and all activity generated through the use of their user ID's and passwords. NASA IT resources, which use passwords for user authentication, will meet the password standards defined in this section. Users will not store passwords in program function keys or automated logon sequences.	
A.6.3.1	Individual Accountability	Providing protection against loss or disclosure of passwords in his or her possession All activity that occurs as a result of deliberately revealing his or her user ID and password

Table 3.2-1. NASA NPG 2810.1 Requirements (3 of 4)

NPG 2810.1 Requirement ID	High Level Requirement Text	Detailed Requirement Text
A.6.3.2	Password Length and Composition Management will ensure that the following password length requirements are implemented:	Minimum of eight characters The eight characters will contain at least one character each from at least three of the following sets of characters: uppercase letters, lowercase letters, numbers, special characters.
A.6.3.3	Password Triviality Management will implement a process to ensure that non-trivial passwords are used on NASA systems. A password is considered nontrivial if it meets the following criteria:	The password is not equal to the user ID. The password is not a dictionary word. The password is not either wholly or predominantly composed of the following: - The user's ID, owner's name, birth date, Social Security Number, family member or pet names, names spelled backwards, or other personal information about the user - Any contractor name - The division or branch name - Repetitive or keyboard patterns (e.g., "abc#abc#", "1234", "qwer", "mnbvc", or "aaa#aaaa") - The name of any automobile or sports team The password is not a word found in a dictionary of any language or a dictionary word with numbers appended or prepended to it. The password is not the name of a vendor product or a nickname for a product.
A.6.3.4	Password Maximum Lifetime Management will ensure that the following password lifetime requirements are implemented	1 year maximum
A.6.3.5	Password Sharing Management will implement a process to ensure that the following password sharing requirements are followed:	Personal passwords used to authenticate identity will be owned (i.e., known) by only the individual having that identity. The user ID owner may employ system features (e.g., logon by or the equivalent) to grant ongoing access to another individual or may create a temporary password.
A.6.3.6	Password Reuse	Stored passwords will be protected in such a way that only the password system is authorized access to a password. Passwords that are encrypted before they are stored will be protected from substitution (i.e., protection will be provided so that one encrypted password cannot be replaced with another unless the replacement is authorized).

Table 3.2-1. NASA NPG 2810.1 Requirements (4 of 4)

NPG 2810.1 Requirement ID	High Level Requirement Text	Detailed Requirement Text
A.6.3.8	Password Distribution Management will implement a password distribution system that accomplishes the following:	Distributes personal passwords in a way that affords reasonable protection from unauthorized disclosure Distributes passwords in such a way that temporary storage of the password is erased, and long-term retention of the password is available only to the owner and the protected password system Ensures that passwords are not visible at the user terminal when being typed Distributes passwords so that an audit record, containing the user ID, date, and time of a password change is maintained and is available only to authorized personnel
A.6.3.9	Password Reset Passwords are reset when a user forgets his or her password, when evidence exists that a password has been compromised, or when management believes a password reset to be in the best interests of the security of the system. Management will implement a process that accomplishes the following:	Confirms name, location, phone number, and system user ID of the user needing reset Provides positive identification of the user ID owner Assigns, at the user's request, a new nontrivial password Ensures that the password is reset by the user during first sign-on
A.6.3.10	Initial Passwords Management will implement a process for generating and assigning the initial password for each user ID. This process will ensure the following:	Removal of all vendor-supplied passwords Assignment of nontrivial initial user password Initial user password is changed during the first logon by the user
A.6.4.3	Controlled Access Protection Controlled access protection is the ability of the system to control the circumstances under which users have access to resources. Management will ensure that all systems that are accessed by more than one user will provide the following controlled access protection when those users do not have the same authorization to use all of the information on the system:	Provides individual electronic accountability through identification and authentication of each system user Provides audit trails or a journal of security-relevant events Provides the ability to control a user's access to information

3.3 ECS Derived (SACM) Requirements

This trade study and evaluation provides an opportunity to expand and improve current security access control management requirements. Instead of specifying specific product capabilities, ECS proposes to refer to the SACM as services. Table 3.3-1 lists SACM derived requirements.

Table 3.3-1. ECS Derived SACM Requirements (1 of 3)

Derived Requirement ID	Derived Requirement Text
Account Management	
D.1.1	The SACM service shall restrict access to specific systems such as trusted hosts. (e.g. DNS and NIS server)
D.1.2	The SACM service shall reduce the number of ECS non-systems administrators having access to accounts system-wide and shall allow all or nothing access to enterprise accounts
D.1.3	The SACM service shall reduce the staff support need to manage user accounts.
D.1.4	The SACM service shall support a web-based GUI.
D.1.5	The SACM service shall keep an audit log of system security events on a separate log host.
D.1.6	The SACM service shall keep an audit log will be accessible to a limited number of system/security administrators.
D.1.7	The SACM service shall maintain a checksums database of often used system commands
Password Changes/Reset	
D.2.1	The SACM service shall allow personnel with limited authorization to perform user password resets.
D.2.21	The SACM service shall eliminate the need for password changes to be performed by system administrator.
D.2.3	The SACM service shall monitor each privileged action on ECS systems.
D.2.4	The SACM service shall provide for keystroke logging.
D.2.5	The SACM service shall force all SA to be accountable for their actions.
D.2.6	The SACM service shall assist the user in selecting either random or user selected passwords with NASA specific character minimums
D.2.7	The SACM service shall provide graceful password aging.

Table 3.3-1. ECS Derived SACM Requirements (2 of 3)

Derived Requirement ID	Derived Requirement Text
D.2.8	The SACM service shall provide the ability to automatically (but temporarily) disable accounts after three bad login attempts
D.2.9	The SACM service shall force a user to change an expired password at their next login
D.2.10	The SACM service shall provide different handling of the root account and passwords
D.2.11	The SACM service shall provide the option of requiring both an SSH pass phrase and a password.
Interactive Access	
D.3.1	The SACM service shall allow only valid users to log into the ECS UNIX environment
D.3.2	The SACM service shall be compatible with F-Secure Secure Shell (ssh)
D.3.3	SACM shall verify current status of a user password.
D.34	The SACM service shall permit or deny access to ECS systems by a specific day of the year.
D.3.6	The SACM service permit or deny user access to ECS systems to a specific day of the l week.
D.3.7	The SACM service shall permit or deny user access to ECS systems to a specific time of the day.
D.3.9	The SACM service shall support limiting user access based on the specific source or target computer, account, time of day and day of the week.
D.3.10	The SACM service shall require that the user password be entered when a privileged command is permitted.
D.3.12	The SACM service shall be capable of recording user keystrokes when a privileged command is permitted and the user is verified.

Table 3.3-1. ECS Derived SACM Requirements (3 of 3)

Derived Requirement ID	Derived Requirement Text
Special Accounts	
D.4.1	The SACM service shall enable a user other than root with the correct authorization to start, stop or backup a Sybase database
D.4.1	The SACM service shall enable a user other than root with the correct authorization to start or stop the AMASS application
Group Account	
D.5.1	The SACM service shall enable each user have privilege delegation.
D.5.2	The SACM service must eliminate the need for group user accounts.
D.5.3	The SACM service shall assign each user an individual account.

This page intentionally left blank.

4. ECS Current Architecture

By design, all interactive access to ECS/EMD systems must be controlled and managed. Privileged access must be auditable. The ECS security architecture consists of a policy-based, three layer model. Figure 2 depicts the ECS Security Architecture:

Perimeter services – The ECS Router and Firewall provide the first line of defense. Only specific protocols and ports are supported inbound:

- Secure Shell
- HTTP
- FTP
- SMTP
- Limited RPC services for V0Gateway support

Access services – ECS/EMD gateway hosts limit the "entrances" to external interfaces. By limiting the services provided and following other hardening and rapid update procedures, maximum protection is provided. Interactive access is limited to least privilege with privileged access audited.

Production services – External access to production hosts has been eliminated. Internal interactive access is limited to least privilege via netgroups with privileged access audited. Access to the archives and write access to the Storage Area Network is controlled via separate netgroups, file/directory permissions and making media read-only as soon as they are full.

The ECS/EMD data archives have been designated a national asset. Therefore, data integrity protection and system availability is a cornerstone of ECS/EMD capability.

Protection against malicious and accidental data destruction must be provided at all levels of access but balanced by the needs of the community to access the data.

Figure 4-1 provides a diagram of the ECS Security Architecture.

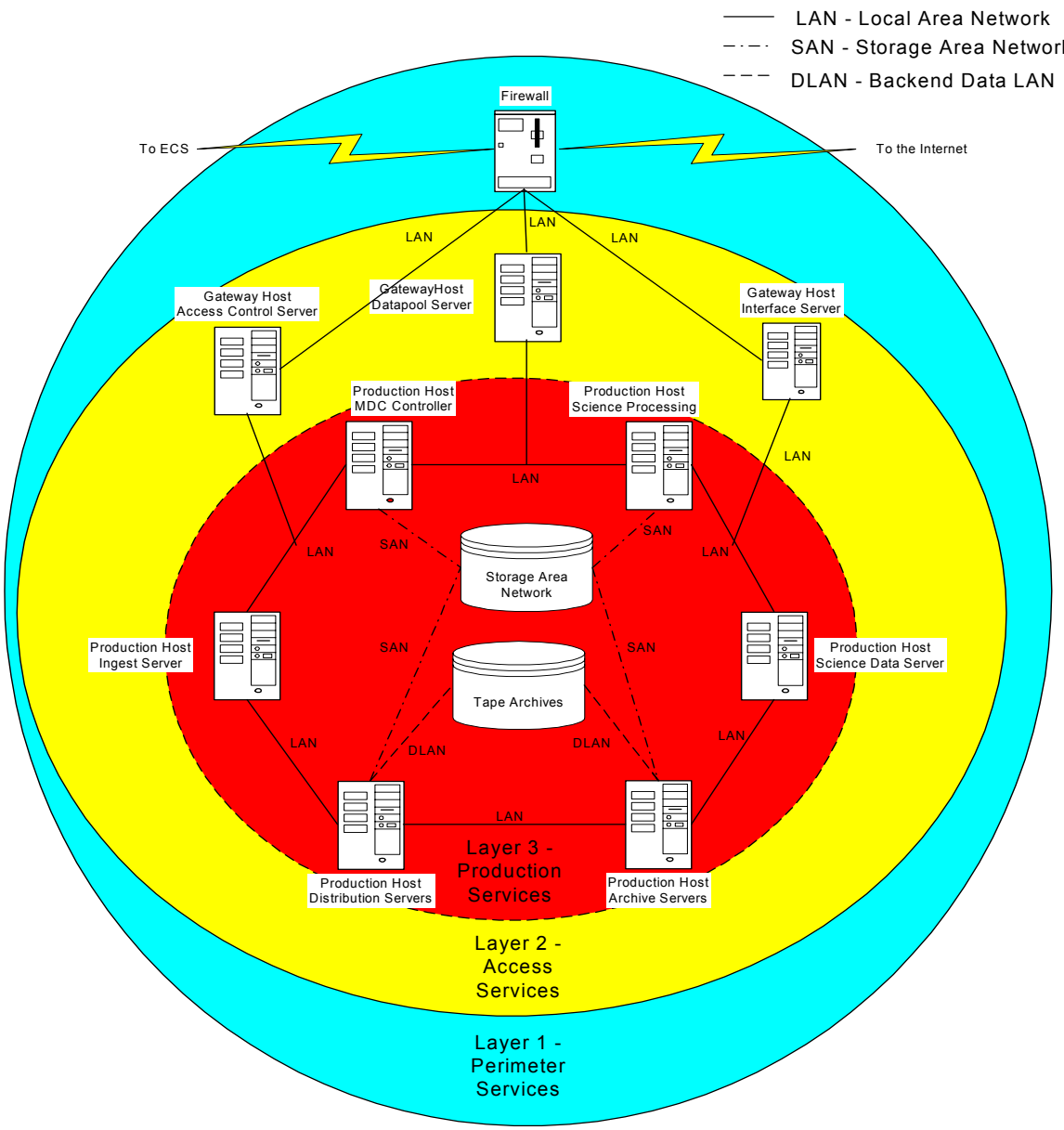

Figure 4-1. ECS Security Architecture

5. ECS Security Access Control Management Operational Scenario

The following subparagraphs describe the current and newly proposed operation scenarios for security access control management.

5.1 Current Operational Scenario

The following subparagraphs provide the current operational scenarios for existing ECS security access control management products.

5.1.1 Account Management

In the area of account management, the System Administrator (SA) using the root account is required to generate or delete new accounts. In an effort to restrict access to particular systems such as trusted hosts, (e.g. network infrastructure management hosts whose function is to determine and maintain trust) requires those systems to be locally managed since the Network Information System (NIS) currently allows all or nothing to system-wide accounts. In practice, this is not often done at the DAACs because of the system management overhead

5.1.2 Password Changes/Resets

At most DAACs, users must change their password every 90 days. Currently, the ANLpasswd freeware application is used to interactively check the new password for compliance with NASA rules. With this product the password resets must be done by an SA since root access is required.

5.1.3 Use of Root account

In a standard UNIX system, root is all-powerful. If there is more than one SA, then accountability is often difficult if not impossible to achieve. The "su –"(substitute user to root) command obviates some of the problems in accountability. However, if the SA has the root password, there is nothing to stop her/him from directly logging in as root, at least at the console. Furthermore, there is no keystroke logging which makes it impossible to track a person's action and hold them accountable.

5.1.4 Interactive Access

ECS has used Secure Shell (ssh) for interactive access for several years, which significantly improve security through strong, encrypted authentication. Each ssh session is logged. When the Portus firewalls were implemented, a policy decision was made to limit the number of DAAC production and M&O hosts that are accessible from the Internet. However, the user is validated on the host itself (i.e. the account is not checked with system security policy). Also, once a valid user is logged in at a "u" (user LAN) host, they may access any UNIX host in that environment.

5.1.5 Special Accounts that Require Root Access

Sybase and AMASS are examples of applications that require root capabilities to start and stop, do backups and perform other maintenance. At the DAACs, only SAs can do these functions. As

a result, this has become an increasingly important issue at the DAACs as they become more independent from the Raytheon/ECS contract.

5.1.6 ECS Group Accounts

The ECS custom software is a complex assembly of client-server applications. ECS Software Development and Systems Engineering have not successfully eliminated the need to use group accounts thereby reducing accountability and increasing risk of system damage due to inadvertent or malicious user action. This is a growing concern at the DAACs.

5.1.7 User Tape Mounts

Normally, operators are not sufficiently privileged to do tape mounts and dismounts so the application must incorporate some difficult twists in order to accomplish this task.

5.2 Proposed New System Operational Scenario

The following subparagraphs provide a detail description of the existing ECS security management process and the proposed incremental changes.

5.2.1 Account Management

The procurement of a new COTS product that has account management features such as account setup, password resets can be delegated to a less skilled, non-root user at the help desk using a web-based GUI. Access to all systems can be included in system policy and managed centrally. For instance, access to trusted hosts running Domain Name Service (DNS) and the Network Information System (NIS) should be limited to SAs. By excluding access in the system policy, normal users would not be permitted to login to trusted hosts.

5.2.2 Password Changes/Resets

The selection of a new security access control management software will include a password change component which will replace ANLpasswd thereby reducing program reliance on one less freeware component. Using the privilege delegation capabilities of the security administration software, Help Desk personnel may be given the capability to reset passwords and thereby save valuable SA time and effort.

5.2.3 Use the Root account

The new security access control management software should minimize the SA need to use the root account. The SAs are given root capabilities when they are required from their own account in a manner similar to the sudo freeware application. Additionally, the session keystrokes used in a privileged command may be recorded for additional accountability/auditability. The keystroke and other logs may be sent to a central log host, which may have restricted access to improve integrity.

5.2.4 Interactive Access

Ssh will complement the security access control management software by first using ssh methods to authenticate the user and then passing on the session to the security access control management software where the system security policy is then enforced. For instance, the

security access control management software will check if the password has expired and if so the user must again authenticate and change their password. After the password check, then it checks that the user has access to this particular host at this particular time of the day and day of the week and if not, then the user is disconnected.

5.2.5 Special Accounts that Require Root Access

The selection of a security access control management tool which supports using the privilege delegation features will allow the DBAs and Archive managers to will be given more direct control of their specialized functions without needing the root password. A keystroke log may be used to record a session when a privileged command is used.

5.2.6 ECS Group Accounts

The selection of security access control management software that has privilege delegation features assigned to individual accounts will eliminate the need for group accounts.

5.2.7 User Tape Mounts

The new security access control management software will allow the operators to be given UNIX tape mount/dismount capabilities using the privilege delegation. A keystroke log may be used to record a session when a privileged command is used.

This page intentionally left blank.

6. SACM Operational Impact Objectives

The following subparagraphs describe the operational impact objectives of a new SACM product on the ECS Core System and its users.

6.1 Impact on Normal Users

The SACM product should have little impact on normal users.

6.2 Impact Privileged Users

Privileged users should no longer need root group account to perform their normal duties.

6.3 Impact on Custom Code

The new SACM product is expected to have little or no impact on the ECS custom code. There should be little configuration needed to integrate the SACM product with the ECS custom code.

6.4 Impact on DUEs

The impact of SACM product on DUEs is very difficult to assess. DUEs vary in complexity from DAAC to DAAC. There is no way for the team to know all of the DUEs that exist at the DAACs. In an effort to ensure that there is minimum impact, we will evaluate the SACM product with known DUEs that has become part of the ECS baseline.

6.5 Impact on Documentation

The SACM product should require a limited number of ECS documents to be updated.

This page intentionally left blank.

7. Security Access Control Management Product Trade Study

This trade study is based upon the ECS system needs analysis, Proposal for Security Requirements Technical Volume, 803-RD-031-001, NASA Policy Guideline 2810.1ECS, and Level 3 Requirements, ECS Security Plan. Based upon these documents, the following selection criteria was used:

1. Unix Multi-Platform Compatibility
2. Cost
3. Ease of Implementation
4. Operating System Supportability
5. Usability
6. Interoperability

7.1 Products Considered

Three products were considered as candidate tools for the security access control management capability. The products are:

1. Tivoli Security Management Module
2. Computer Associates eTrust Access Control
3. Symark PowerPassword and PowerBroker Suite

The following subparagraphs provide an overview of the products.

7.1.1 Tivoli Security Management Module

IBM Tivoli Access Manager for Operating Systems is a policy-based access control system for UNIX and Linux operating systems. This comprehensive security solution effectively addresses the many system vulnerabilities surrounding UNIX/Linux super user or "root" accounts. Many security failures in UNIX/Linux environments are from super user account abuse, or a hack that results in gaining access to this account.

7.1.2 Computer Associates eTrust Access Control

eTrust Access Control is and Enterprise capable system security manager. Its strength is reducing the power of "root" by delegating functions to the users that need the privileges.

7.1.3 Symark PowerPassword and PowerBroker Suite

7.1.3.1 PowerPassword

PowerPassword manages login and password policies across heterogeneous UNIX environments while keeping a centralized, indelible audit trail of all login activity. Symark PowerPassword's security capabilities are the perfect complement to NIS and LDAP environments that require

greater password strength, login constraints, and auditing capabilities. In addition to creating a more secure UNIX environment, PowerPassword reduces help desk support costs with features such as password reset and synchronization.

7.1.3.2 PowerBroker

PowerBroker provides selective delegation of UNIX administrative privileges for trusted users without providing full root access, reducing the risk of accidental damage or malicious activity. PowerBroker also manages privileges and access to third-party applications and accounts (e.g. database, CRM, ERP) including generic accounts.

7.2 Trade Study Selection Criteria

One of the main concerns in this trade study is to limit the impact of SACM product on the ECS Core System.

There are basic requirements that are necessary and can be considered as 'pre-qualifying' and warrant a buy/no-buy decision.

- Support for multi-tiered and multi-OS environments.
- Multiple storage device interfaces.
- Must be easily be integrated into the ECS environment
- Cannot cause any degradation to the ECS environment and custom code.
- Product life cycle cost no more than $300K.
- Product vendor support is based on OS upgrades.

The following sections describe the selection criteria in more detail.

7.2.1 Unix Multi-Platforms Compatibility

Rationale/Reason: ECS has a heterogeneous Unix Environment. The product needs to be compatible with Sun, Linux, and SGI platform. The information provided in the product specification data sheet will serve as valuable information in the evaluation platform compatibility issues.

Each of the trade study alternatives was evaluated based on their respective specification data sheet.

Scoring: Linear score 0 or 10: The product that is compatible with the ECS platforms received a score of 10.

7.2.2 Cost

Rationale/Reason: Cost is divided into three areas: non-recurring, recurring and life cycle. The three COTS products cost's were compared against each other and evaluated for life cycle and maintenance cost.

Scoring: Linear score 1-10: The COTS product with the least cost for life cycle and maintenance support scores the highest.

7.2.3 Ease of Implementation

Rationale/Reason: *Realistic cost and elapsed time for installation can be determined by evaluating the ease of implementation. (e.g. availability of an installation GUI adds to its ease of implementation)*

A system administrator and/or systems engineer evaluated each alternative. The system administrator installed and configured the product in a COTS evaluation designated area within the ECS environment. The systems engineer reviewed the product specification data sheet and held discussions with each product-marketing representative.

Scoring: Linear score 1-10: The product that is the easiest to install and configure, scores the highest.

7.2.4 Operating Systems Supportability

Rationale/Reason: The product must support the current ECS environment baseline (Sun, Linux, SGI) and future level of operating systems. The vendor should have a plan for continued support based on OS upgrades.

As the ECS environment continues to evolve, a product must remain current with the changes in the vendor's operation system changes.

Each of the trade study alternatives were evaluated based on the their respective data specification sheet. In addition, lengthy discussions were held with product marketing representative.

Scoring: Linear score 1-10: The product that stays current with the vendors operating system, scores highest.

7.2.5 Usability

Rationale/Reason: Usability of the product is important because the skill level of system administrators varies at each DAAC. The DAAC personnel need this information to plan for determining the skill level needed to support and maintain the product.

The trade study alternatives were evaluated based on the information gathered from their specification data sheet and the result from the evaluation team.

Scoring: Linear score 1-10: The product that required the least skilled personnel, scores the highest.

7.2.6 Interoperability

Rationale/Reason: It is crucial that the product integrates and interoperates with the ECS custom code. The product must not break the current custom code and must provide a seamless integration into the ECS environment. Impacts to the ECS environment should be kept to a minimum.

Each of the trade study alternatives was evaluated based on the data provided in the specification data sheet and interviews with product marketing representative. In addition results from the product evaluation was considered.

Scoring: Linear score 1-10: The product that integrates and interoperates with the ECS custom code without requiring a substantial amount of work scores the highest.

7.3 Relative weighting and scoring

Table 7.3-1 provides a summary of the relative weighting and scoring used for each of the alternatives considered.

Table 7.3-1. Summary Evaluation Scoring

Selection Criteria	Units	Scoring Range	Criteria Weighting
Unix Multi-Platforms Compatibility	Linear	0 or 10	25%
Cost	Linear	1-10	25%
Ease of Implementation	Linear	1-10	15%
Operating Systems Supportability	Linear	1-10	10%
Usability	Linear	1-10	10%
Interoperability	Linear	1-10	15%

Rationale for the relative weights given for each of the selection criteria:

Unix Multi-Platforms Compatibility: The COTS product is compatible with different Unix platforms in the ECS environment. The weighting is 25% to reflect the importance of multi-platforms compatibility.

Cost: Startup and maintenance costs must be feasible. The weighting is 25% to reflect equal to that of platform heterogeneity.

Ease of Implementation: Past experience with deployment of new COTS products indicates that DAACs will not use any product that requires tremendous amount of overhead to install, configure and maintain. The weighting is 15%.

Operating Systems Supportability: An indication of how the product keeps pace with OS upgrades. The weighting is 10%.

Usability: The ease of use of the tool, either by command line or a GUI if applicable. The weighting is 10%.

Interoperability: An indication of the products ability to integrate and interoperate with ECS custom code and other security COTS presently in the ECS environment. The weighting is 15%.

7.4 Trade Study Evaluation

The scores for each of the products were multiplied by their weighting factor to determine the weighed score for each of the criterion. Table 7.4-1 depicts the raw, weighted, and total weighted score for each product.

Table 7.4-1. Raw, Weighted, and Total Summary Evaluation Scoring

Selection Criteria	Tivoli			CA eTrust			Symark		
	Weighting	Raw Score	Weighted Score (Max=10)	Weighting	Raw Score	Weighted Score (Max =10)	Weighting	Raw Score	Weighted Score (Max =10)
Unix Multi-Platforms Compatibility	25	0	0	25	10	2.5	25	10	2.5
Cost	25	5	1.25	25	4	1	25	9	2.25
Ease of Implementation	10	3	0.3	10	4	0.4	10	7	0.7
Operating Systems Supportability	10	3	0.3	10	4	0.4	10	7	0.7
Usability	15	3	0.45	15	6	0.9	15	8	1.2
Interoperability	15	5	0.75	15	6	0.9	15	9	1.35
Total Weighted Score			**3.05**			**6.1**			**8.7**

7.5 Sensitivity Analysis

The sensitivity of the results to variations in criteria and weighting will identify any variances in the results and help validate the choice. There was a large difference in results between the three alternatives; the Symark Suite is clearly the winner. In this trade study with six factors considered, variations would not have changed the results because of the low score for the multi-platform compatibility, cost, and Interoperability. In addition, the other alternatives ease of implementation and operating systems support were identified as shortcomings.

To check the sensitivity, each criterion was individually zeroed out. The overall results remained the same for each case. This indicates that one criterion did not drive the results. Varying the weighting for the criteria could change the results, but it would be a very unusual weighting ratio that achieves this result. Once again, the Symark Suite product wins. The affect of the other criteria was not enough to offset most variations in weighting.

7.6 Trade Study Conclusion

Symark powerbroker and powerpassword suite was the unanimous winner in the trade analysis. These products outscored the other products.

This page intentionally left blank.

8. Security Access Control Management Product Cost Comparison

The life cycle cost for the product was important factor criteria used in the trade analysis. The subparagraphs provide the cost of security access management products considered.

8.1 Cost Comparison of COTS Products

The comparison cost for Tivoli Security Management Module, CA eTrust and Symark Suite comparison are given in Table 8.1-1 below.

Table 8.1-1. Cost Comparisons of COTS Products

Estimated Cost and Schedule of:	Tivoli Security Management Module	CA eTrust	Symark Suite
Cost per Server (Average for quantity 19)	9,000.00	8,100.00	4,000.00
Cost for 6 Sites	171,000.00	153,900.00	76,000.00
Total Life-cycle Cost (including Maintenance)	205,200.00	162,000.00	104,800.00
Total Implementation Schedule	12months	9 months	6 months

NOTE 1: Tivoli and eTrust costs are estimated from previous quotes. More current quotes will be obtained if required.

N0TE 2: The cost stated in the table does not include subcontractor fees.

This page intentionally left blank.

9. Security Access Control Management Product Technical Evaluation

9.1 Tivoli Security Management Module

Tivoli Security Management software OEM'd the SEOS tool and put the Tivoli Enterprise Management (TEM) framework around it. However, Tivoli has only supported the SGI IRIX as a third tier operating system, which translates to rather poor support and currently does not support an SGI Security Management Module client with the TEM. TEM is an extremely powerful and flexible system -- and very hard in terms of expertise and time to install, learn and maintain. DAAC resistance to that level of effort has led to the removal of TEM from the ECS baseline. When the suggestion to use the Tivoli Security Management Module at the DAACs during a recent DAAC quarterly meeting, the idea was immediately and unanimously rejected.

The evaluation group's determination was that Tivoli Security Management Module was not a viable alternative

9.2 Computer Associates eTrust Access Control

The CA eTrust Access control product is designed to bring improved account management and resource management. Product development was initiated in the 1980's by several ex-IBM programmers who had been asked to port/develop an IBM-mainframe security package called RACF (Remote Access Facility) to UNIX and called it SEOS (Security Enhanced Operating System).

The basic concept was to insert a thin security layer between the system kernel and security-based system calls. That layer trapped all security related system calls and sent them off to a database that had a set of security policy rules. From there, SEOS determined if the requesting application had the necessary privileges to access that command or data. Access was permitted or denied as stated in security policy. The user is not aware of the operation of the security application. Each host must have the server product software installed. There is no client/server operation as there is on other products. Since the product is expensive, it was originally thought that only the NIS servers would host the software and all other hosts would run a network-based remote command to change/update passwords. This significantly reduces the overall cost of the system but only helps the system security at the NIS servers and not the other systems.

In the intervening years, the control of the company has changed hands twice, which has caused a noticeable change in emphasis. UNIX is no longer the target environment - Microsoft Windows is. This was noticeable during the product evaluation last year. The CA claim was that SGI IRIX and Sun Solaris were supported, but after four weeks of effort, neither OS worked as advertised. Furthermore, there was no indication when the testing was stopped that success was near at hand.

The evaluation group's determination was that CA eTrust was not a viable alternative.

9.3 Symark PowerPassword and PowerBroker

The following subparagraphs describe the evaluation of the PowerPassword and PowerBroker security access control management COTS product.

9.3.1 Symark PowerPassword and PowerBroker Operational Impact

9.3.1.1 Impact on Normal Users

Most users will not notice that there is anything new that happening on the system unless they let their passwords expire. Also, should the DAACs decide to limit access from one or more hosts, and then a "normal" user may not be able to access that system

9.3.1.2 Impact Privileged Users

People responsible for tasks that are normally run by root will be able to use their own accounts rather than a group account such as root, Sybase or AMASS. To execute a privileged application, prepend it with "pbrun". So to mount a tape might use a command:

% pbrun mount /dev/rmt/0 <enter>

9.3.1.3 Impact on Custom Code

No changes to the custom code *itself* are required. However, if PowerBroker is used, the prefix command “pbrun” (short for powerbroker run) must be added to the startup scripts for each of the servers. This is needed to make “cmshared” or “allmode” the owner of the process rather than an individual user. The change can be done easily and quickly and has been verified to work during the course of testing. It must be remembered that merging of these alternate startup scripts is required.

9.3.1.4 Impact on DUEs

No changes to the DUEs themselves should be required. However, if PowerBroker is used, the startup scripts will need to be changed to add a prefix command “pbrun”. This is required to make “cmshared” or “allmode” the owner of the process rather than an individual user. The change should be straightforward to implement.

9.3.1.5 Impact on Documentation

The following documents will be updated to reflect the integration of the new SACM product.

- 611-CD-610 Mission Operation Procedures
- 609-CD-610 Operation Tool Manual

9.3.2 PowerPassword Evaluation

An evaluation of the Symark PowerPassword product was conducted on the PVC prototype LAN at the Raytheon facility in Landover, Maryland in May and June 2003. PowerPassword provides a robust interactive access control system to a significantly higher level of sophistication than is presently possible. It would replace the existing ANLpasswd functionality. The product was evaluated on the three types of operating systems that are baselined in ECS – Sun Solaris 8, SGI

IRIX 6.5, and Red Hat 7.3. F-Secure Secure Shell (ssh) 3.2 was installed on the test hosts in order to evaluate ssh/PowerPassword integration.

The first installation was accomplished on a Linux host with the assistance of a Symark engineer and went very smoothly. Systems Engineering and RTSC personnel accomplished the other installations. The installation also went well. Each installation took less than an hour to complete. The installation technique is Symark-specific. (i.e., they do not use a Solaris "pkgadd", Linux "rpm", or IRIX "inst" packages.) A license string is required for each primary or backup server. Clients do not require a license string but the installation process is the same. There appears to be a method of automating the installation process by recording the selections made on the initial installations but this was not attempted.

After an installation, the configuration for security policies is straightforward. On a per user basis, it is possible to:

- Permit/deny host access – Some hosts (such as infrastructure hosts) may be made "off-limits" to all but system administrators. This is a major improvement over NIS where access is all-or-nothing. This capability will be useful in strengthening overall security.
- Time of day restrictions – Users can be restricted to normal work hours if necessary.
- Terminated or expired accounts – If a user leaves the program, access to the account can be terminated from one location. This may be done on a schedule also (i.e. in advance).
- Password expiration – PowerPassword takes the login "handoff" from ssh and will enforce password policy *even if public key authentication is used*. That is, if a user uses their passphrase to login to a system and the password has expired, the user must change the password successfully before the user may logon. This eliminates one of the few shortcomings of ssh.
- Password update enforcement – The NPG 2810 requirement to update passwords every 90 days is enforced using policy.
- Password characteristics – The NPG 2810 requirement to be at least 8 characters, use of numeric and special characters is enforced by policy. Note that there is an additional perl module that will be required in order to do dictionary checks as required by NPG 2810. The "hook" is in the PowerPassword software for an external checker but is not part of the application.

The only changes required to integrate ssh 3.2 are uncommenting the following two standard lines in the ECS version of the /etc/ssh2/sshd2_config file:

ExternalAuthorizationProgram	/usr/local/bin/ppext_authorize
PasswdPath	/usr/local/bin/pppasswd

In order for PowerPassword to work, a host is designated as the primary server. All changes to policy are done at the primary server. For redundancy, at least one backup server should be implemented. Changes in policy are automatically downloaded to each backup server. Any server may then respond to client login requests. It is expected that LP DAAC, LaRC DAAC, GES DAAC and the PVC will require three servers (one primary and two backups). Two servers should be sufficient for NSIDC DAAC, the SMC and the VATC (one primary and one backup). The servers will be added to existing infrastructure hosts. It is desirable to implement a security

loghost that could be shared with PowerBroker -- especially if one can be “recycled” from existing hardware.

Both Linux and Solaris hosts were used successfully as primary and backup servers. Linux, Solaris and IRIX were used successfully as clients.

PowerPassword was tested both with and without ssh 3.2 integration successfully. Additional tests included password update enforcement and password characteristics. All of the tests in PowerPassword were successful on each platform.

9.3.3 PowerPassword Test Case Scenarios and Results

Table 9.3.3-1 consists of the test scenarios used during the evaluation of PowerPassword.

Table 9.3.3-1. PowerPassword Test Scenarios and Results (1 of 2)

Case Reference	Command	Expected Results	Pass	Fail
01 – Permit/deny host access.	in /etc/ppserv.settings if (user=="bpeters" && host=="toccata" accept; deny;	**user bpeters may login to host toccata but others rejected**	yes	
02- Time of day restrictions	in /etc/ppserv.settings weekdays={"Mon", "Tue", "Wed", "Thu", "Fri"}; if (user=="pptest" && host=="sparky" && timebetween(800, 1700) && dayname in weekdays) accept;	user pptest may login to host sparky during normal business hours but others rejected	yes	
03- Terminated or expired accounts	in /etc/ppserv.settings if (user=="badguy") deny;	disallow user badguy anywhere	yes	

04-. Password expiration	in /etc/ppserv.settings
	if(pwmaxage > 0)
	{
	if(pwmaxage - pwage < warndays)
	{
	requestpwchange();
	}
	}
	accept;
		if the password maximum age is greater than 0 and the password age is less than the number of days until mandatory change, allow the login.	yes	

Table 9.3.3-1. PowerPassword Test Scenarios and Results (2 of 2)

Case Reference	Command	Expected Results	Pass	Fail
05- Password update enforcement	in /etc/ppserv.settings if(pwmaxage > 0) pwage < warndays) requestpwchange ();	If the password age is less than the number of warning days, change the password.	yes	

06- Limit host access to specific groups	in /etc/ppserv.settings:
	# developers may log in to development hosts only
	if(group == "dev" && isadevhost)
	accept;
		developers in the group "dev" may login to hosts that are in the development group are permitted to login.	yes	

07 – Use NIS netgroups to permit/deny access	if(!innetgroup ("myhosts", host)) reject; accept;	Get the netgroup myhosts from NIS and reject if not in the group and accept if the user is in the group	yes	

In summary, PowerPassword is a very straightforward application that will provide a significant improvement in controlling access to ECS systems.

9.3.4 PowerBroker Evaluation

Symark PowerBroker was evaluated in parallel with PowerPassword. Powerbroker solves the function delegation problem that has been difficult as the transition towards DAAC independence has progressed. UNIX is designed around the root account as being "all powerful". It is often useful in operations, however, to assign different privileged tasks to different users and that is what PowerBroker does. It does not require any changes to the operating system kernel and works within user space. In operation it is like the "sudo" program in that the prefix "pbrun" is used when a user needs to invoke a privileged function. So in order to run a mount command (normally only executable by root), the user would type:

% pbrun mount /dev/rmt0 <enter>

PowerBroker is designed to work with DNS, NIS, NIS+, and LDAP. For the evaluation, it worked well with the existing infrastructure. Otherwise, there are no prerequisites.

The first installation was accomplished on a Linux host with the assistance of a Symark engineer (on a separate date than the PowerPassword install) and went very well. The other installations were accomplished by Systems Engineering and RTSC personnel and also went well. Each installation took about an hour to complete. The installation technique for PowerBroker is Symark-specific. (i.e., they do not use a Solaris "pkgadd", Linux "rpm", or IRIX "inst" packages.) A license string is required for each master server. Clients do not require a license string but the installation process is the same. There appears to be a method of automating the installation process by recording the selections made on the initial installations but this was not

attempted. The installation process and the documentation structure is slightly different between the two packages which was mildly annoying. Symark reports that they are attempting to make the processes more homogeneous.

PowerBroker uses three types of hosts – a *submit* host which is the system that requests a policy check on a command, an *accept* host which does the policy check and a *run* host which is an optional third host where the command may be executed. A single host may be one or all types. A submit host acts like a client in PowerPassword and does not need a license string. It is expected that LP DAAC, LaRC DAAC, GES DAAC and the PVC will require three accept hosts. Two accept hosts should be sufficient for NSIDC DAAC, the SMC and the VATC. The servers will be added to existing infrastructure hosts. It is desirable to implement a security loghost that could be shared with PowerPassword -- especially if one can be "recycled" from existing hardware.

All changes to policy are done at an accept host. For redundancy, at least two accepts hosts should be implemented. Any accept host may then respond to submit host requests.

Linux, Solaris and IRIX systems were used successfully as submit and accept hosts.

The command reference manual is about two inches thick and not all of the commands were verified. The evaluation team felt it was sufficient that the capabilities listed above were all achievable with commands with which the evaluators became familiar. Symark has cleverly packaged example scripts that are very helpful in learning how to use the product. The script language is very "C compiler" like and therefore fairly easy for most system administrator types to at least understand and in most cases implement.

9.3.5 PowerBroker Test Case Scenarios and Results

Table 9.3.5.1 consists of the test scenarios used during the evaluation of PowerBroker.

Table 9.3.5-1. Power Broker Test Scenarios and Results (1 of 2)

Case Reference	Command	Expected Results	Pass	Fail
01 – The user cmshared cannot log into an xterm workstation as cmshared.	./builder cmshared policy would be set on host.	The user would be prompt to log in as valid lab user.	yes	
02- The PVC users can only su (switch user) to cmshared using pbrun with audit log enabled.	./pbrun cmshared	The user should be prompt to enter password and audit log should be enable.	yes	
03- When a user su (switch user) to cmshared, the keystrokes can be logged and monitored.	Edit the /etc/pb/io_logging.conf file and add cmshared	The user would be prompt to enter current password and will be switched to cmshared.	yes	

Table 9.3.5-1. Power Broker Test Scenarios and Results (2 of 2)

Case Reference	Command	Expected Results	Pass	Fail
04- The user is identified when su (switch user) to cmshared.	./pbrun cmshared	In the /var/log directory a log file is generated	yes	
05- The user cmshared can have only one email configuration.	./builder cmshared policy would be set on host.	The cmshared email configuration cannot be changed.	yes	
06- Limit lab users to su (switch user) to cmshared instances.	./builder cmshared policy would be set on host.	A limited instances of cmshared is set i.e., Ingest =(2)	yes	
07- Grant lab users cmshared privileges.	./builder cmshared policy would be set on the host.	Lab user will be able to execute commands the would normally be performed by cmshared	yes	
08- A limited ability to shutdown or reboot hosts/servers.	./builder cmshared policy would be set on the host.	In the event of an emergency the cmshared account will have the ability to reboot host/servers.	yes	
09- Prevent the security exploit of the pbrun program.	This would be done when installing and configuring of program.	Users cannot use the sudo vi security exploit in sudo.	yes	
10- Create an emergency root user that does have access to any hosts or servers	./builder cmshared Policy would be set on host.	The password will be kept by a non-lab user (Lab Lead) if an emergency arises the two user must collude to subvert the system security.	yes[1]	
11- Make lab lead or Responsible Engineer (RE) the emergency root user	./builder *abuser policy would be set on host*.	This user is for emergency root user.	yes	

PowerBroker is a much more involved application, so there were additional items that the team could have evaluated if time had permitted.

In summary, PowerBroker is a product that will improve ECS operations by the elimination of most (if not all) group and application accounts. This alone will make it worth the effort to deploy.

This page intentionally left blank.

10. Recommendation

ECS recommends Symark PowerPassword and PowerBroker as the security access control products. The Symark products will improve the current ECS security access control management process and enchance our ability to meet the long-term goals. The following factors contributed to this recommendation.

1. An assessment of the EDF, DAACs and SMC security control management needs.
2. Requirements Analysis of all of the security access control management requirements on the ECS program.
3. A trade study of the COTS products considered.
4. An evaluation of the COTS products considered
5. The other COTS product vendors required two or three servers per site. The Symark product enables all of the systems to be protected instead of just the three servers thus significantly improving the value of the product to the program.
6. The life-cycle cost for the Symark product is $105K for production.
7. The implementation schedule for the Symark product is shorter than the other vendors, therefore allowing us to expedite the deployment to the sites
8. Operational Impact of the Symark PowerPassword and PowerBroker products on ECS.
9. The Symark products are viable candidates for implementation cross ECS program including M&O servers.

This page intentionally left blank.

11. Future Trade Study and Evaluation

This white paper addressed security access control management for the ECS UNIX environment only. If there is a need to perform a similar study and evaluation for the PCs and the Maintenance and Operational resources environment, we will require direction and funding from ESDIS.

This page intentionally left blank.